DETAILED ACTION

1. This office action is in response to the communication filed on 06/11/2010.

2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

3. Claims 1-28 and 30-34 were pending in the application.

4. Claim 10 is cancelled in examiner's amendments made in this office action.

5. Claims 1-9, 11-28 and 30-34 are allowed.

RESPONSE TO ARGUMENTS

6. Applicant's arguments regarding objections to claim 13 are fully considered, the previous objections to claim 13 are withdrawn because of the amendments made to the claim.

7. The applicant's arguments regarding 35 USC 103(a) type rejections are fully considered, and found persuasive. The previous 35 USC 103(a) type rejections are withdrawn based on the applicant's arguments, and the examiner's amendments made to the claims in this office action.

EXAMINER'S AMENDMENT

8. An examiner's amendment to the record appears below. Should the changes and/ or additions be unacceptable to the applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. Authorization for this examiner's amendment was given in a telephone interview with the applicant's representative Mr. Brian Genco on June 16, 2010.

Claims 1, 9, 10, 28 and 34 have been amended as follows:

Claim 1. (Currently Amended) A system to provide application-to-application enterprise security for different applications on different platforms where there is no continuing context or session and a new context is created with new invocations from one of the applications to another, the system comprising:

a first computer comprising a security application program interface and an application program interface coupled to a client application on a first platform, the security application program interface operable to provide a security credential;

an authentication authority receiving the security credential from the security application program interface, the authentication authority further generates a token and communicates the token to the security application program interface where the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent string data type;

a store maintaining data validating the security credential, the store in communication with the authentication authority to validate the security credential,

the application program interface coupled to the client application communicating regarding the validity of the token; and

a second computer comprising a distinct server application on a second platform to receive the token from the application program interface coupled to the client application, a security application program interface coupled to the distinct server application communicating with the authentication authority to validate the token to enable the client application to use services of the server application, wherein there is no continuing context or

session and a new context is created with every invocation of ~~functionality~~ service of the distinct server application by the client application.

Claim 9. (Currently Amended) A method for providing application-to-application enterprise security for different applications on different platforms where there is no continuing context or session and a new context is created with new invocations from one of the applications to another, the method comprising:

coupling a security application program interface and an application program interface to a client application on a first platform;

communicating a security credential from the security application program interface to an authentication authority;

communicating information related to the security credential between the authentication authority and a data store to determine whether the security credential is valid;

generating a token by the authentication authority when the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent string data type;

communicating the token to a security application program interface of the client application;

providing, by the application program interface coupled to the client application on the first platform, the token to a distinct server application, the distinct server application on a second platform, wherein there is no continuing context or session and a new context is created with each of a plurality of invocations of ~~functionality~~ service of the distinct server application by the client application; and

~~validating~~ communicating, by a security application program interface coupled to the distinct server application, with the authentication authority to validate the token before providing access to services of the distinct server application by the client application.

Claim 10. (Canceled)

Claim 28. (Currently Amended) A system to provide application-to-application enterprise security for different applications on different platforms where there is no continuing context or session and a new context is created with new invocations from one of the applications to another, the system comprising:

a first computer comprising a first application program interface coupled to a first application on a first platform and a first security application program interface coupled to the first application on the first platform, to provide a first security credential;

a first security application program interface coupled to the first application on the first platform, to provide a first security credential;

a second computer comprising a second application program interface coupled to a second application on a second platform and a second security application program interface coupled to the second application on the second platform, to provide a second security credential;

an authentication authority receiving the first and second security credentials from the first and second security application program interfaces, the authentication authority further generating tokens and communicating the tokens to the first and second security application program interfaces where the first and second security credentials are valid, wherein the

tokens contain user credentials encoded as a platform and application independent string data type, wherein the tokens generated by the authentication authority are further defined as a first token generated by the authentication authority for the first application based on the first security credential and a second token generated by the authentication authority for the second application based on the second security credential;

a store maintaining data validating the first and second security credentials, the store in communication with the authentication authority to validate the first and second security credentials;

the first application program interface communicating regarding tokens; and

the second application program interface receiving the first token from the first application program interface, wherein there is no continuing context or session and a new context is created with [[an]] each invocation of the second application program interface by the first application program interface, the second security application program interface communicating with the authentication authority to validate the first token to enable the first application to use services of the second application and wherein the first application program interface receives the second token from the second application program interface, wherein there is no continuing context or session and a new context is created with [[an]] each invocation of the first application program interface by the second application program interface, the first security application program interface communicating with the authentication authority to validate the second token to enable the second application to use services of the first application.

Claim 34. (Currently Amended) The system of Claim 1, wherein the invocation of ~~functionality~~ service is an invocation of a method.

EXAMINER'S REASONS FOR ALLOWANCE

9. The following is an examiner's statement of reasons for allowances:

Independent claim 1 is patentable over the cited prior arts because independently or in combination, they do not anticipate nor fairly and reasonably teach a system to provide application-to-application enterprise security for different applications on different platforms where there is no continuing context or session and a new context is created with new invocations from one of the applications to another, the system comprising besides other components: an authentication authority receiving the security credential from the security application program interface, the authentication authority further generates a token and communicates the token to the security application program interface where the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent string data type; and a second computer comprising a distinct server application on a second platform to receive the token from the application program interface coupled to the client application, a security application program interface coupled to the distinct server application communicating with the authentication authority to validate the token to enable the client application to use services of the server application, wherein there is no continuing context or session and a new context is created with every invocation of service of the distinct server application by the client application.

Independent claim 9 is patentable over the cited prior arts because independently or in combination, they do not anticipate nor fairly and reasonably teach a method for providing application-to-application enterprise security for different applications on different platforms where there is no continuing context or session and a new context is created with new invocations from one of the applications to another, the method comprising besides other features: communicating a security credential from the security application program interface to an authentication authority; and communicating information related to the security credential between the authentication authority and a data store to determine whether the security credential is valid; and generating a token by the authentication authority when the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent string data type; and providing, by the application program interface coupled to the client application on the first platform, the token to a distinct server application, the distinct server application on a second platform, wherein there is no continuing context or session and a new context is created with each of a plurality of invocations of service of the distinct server application by the client application; and communicating, by a security application program interface coupled to the distinct server application, with the authentication authority to validate the token before providing access to services of the distinct server application by the client application.

Independent claim 28 is patentable over the cited prior arts because independently or in combination, they do not anticipate nor fairly and reasonably teach a system to provide application-to-application enterprise security for different applications on different platforms where there is no continuing context or session and a new context is created with new

invocations from one of the applications to another, the system comprising besides other components: a first computer comprising a first application program interface coupled to a first application on a first platform and a first security application program interface coupled to the first application on the first platform, to provide a first security credential; and a second computer comprising a second application program interface coupled to a second application on a second platform and a second security application program interface coupled to the second application on the second platform, to provide a second security credential; an authentication authority receiving the first and second security credentials from the first and second security application program interfaces, the authentication authority further generating tokens and communicating the tokens to the first and second security application program interfaces where the first and second security credentials are valid, wherein the tokens contain user credentials encoded as a platform and application independent string data type, wherein the tokens generated by the authentication authority are further defined as a first token generated by the authentication authority for the first application based on the first security credential and a second token generated by the authentication authority for the second application based on the second security credential; and a store maintaining data validating the first and second security credentials, the store in communication with the authentication authority to validate the first and second security credentials; and the second application program interface receiving the first token from the first application program interface, wherein there is no continuing context or session and a new context is created with [[an]] <u>each</u> invocation of the second application program interface by the first application program interface, the second security application program interface communicating with the authentication authority to validate the first token to enable the first application to use

services of the second application and wherein the first application program interface receives the second token from the second application program interface, wherein there is no continuing context or session and a new context is created with each invocation of the first application program interface by the second application program interface, the first security application program interface communicating with the authentication authority to validate the second token to enable the second application to use services of the first application.

Dependent claims are allowed because of their dependencies on the allowable independent claims.

CONCLUSION

10. Claims 1-9, 11-28 and 30-34 are patentable.

11. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays should be clearly labeled "Comments on Statement of Reasons for Allowance."

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M. Z. Abedin

Examiner, A.U. 2436

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436